Государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа с. Чёрный Ключ муниципального района Клявлинский Самарской области

Проверено
Заместитель директора по ВР
_____/Семенова Т.И./
«30» августа 2024 г.

Утверждено приказом № 74/1 – од
Директор_____/Ильина В.В

«30» августа 2024 г.

Ильина В.В.

Ильина В.В.
О=ГБОУ СОШ с.Чёрный Ключ, CN=Ильина В.В., E=so_svu_ch_klyuch_sch@samara.edu.ru
Я являюсь автором этого документа
2024.09.05 22:20:19+04'00'

РАБОЧАЯ ПРОГРАММА
внеурочной деятельности «Информационная безопасность»
основного общего образования
Направление: общеинтеллектуальное

Рассмотрена на заседании МО гуманитарного цикла
Протокол № 1 от 30.08.2024г
Руководитель МО_____/Купряева Е.А./
подпись (ФИО)

Планируемые результаты освоения курса внеурочной деятельности «Информационная безопасность»

№	Название раздела (темы)	Планируемые результаты		
		личностные	предметные	метапредметные
1.	Безопасность общения	• осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников; • готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных	Ученик научится: • анализировать доменные имена компьютеров и адреса документов в интернете; • безопасно использовать средства коммуникации; • безопасно вести и применять способы самозащиты при попытке мошенничества; • безопасно использовать ресурсы интернета. Ученик получит возможность научиться: • соблюдать нормы информационной этики и права; • самоконтролю, самооценке, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности; • решению использовать коммуникативные задачи в области безопасности жизнедеятельности различных источников информации, включая Интернет- ресурсы и другие базы данных.	Регулятивные: • идентифицировать собственные проблемы и определять главную проблему; • выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат; • ставить цель деятельности на основе определенной проблемы и существующих возможностей; • выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели; • составлять план решения проблемы (выполнения проекта, проведения исследования); • описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса; • оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата; • находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата; • работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата; • принимать решение в учебной ситуации и нести за него ответственность. Познавательные: • выделять явление из общего ряда других явлений; • определять обстоятельства, которые предшествовали
2.	Безопасность устройств			
3.	Безопасность информации			

		интересов; • освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах; • сформированность понимания ценности безопасного образа жизни; • интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.		возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений; • строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям; • излагать полученную информацию, интерпретируя ее в контексте решаемой задачи; • самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации; • критически оценивать содержание и форму текста; • определять необходимые ключевые поисковые слова и запросы. Коммуникативные: • строить позитивные отношения в процессе учебной и познавательной деятельности; • критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его; • договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей; • делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его; • целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ; выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации; использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для

				решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.; • использовать информацию с учетом этических и правовых норм; • создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.
	Итого: 34 ч.			

Содержание курса внеурочной деятельности «Информационная безопасность»

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Тема 2. С кем безопасно общаться в интернете. Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Тема 3. Пароли для аккаунтов социальных сетей. Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях. Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях. Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты. Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

Тема 9. Фишинг. Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах. Выполнение и защита индивидуальных и групповых проектов.

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода. Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Тема 3. Методы защиты от вредоносных программ. Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Тема 4. Распространение вредоносного кода для мобильных устройств. Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Тематическое планирование по курсу внеурочной деятельности

«Информационная безопасность» 7и 8 класс

№	Название темы	Количество часов
1	Безопасность общения	12
2	Безопасность устройств	8
3	Безопасность информации	14
	ИТОГО	**34**